UNT SYSTEM

2022

Information Security Handbook

University of North Texas System
University of North Texas
University of North Texas Health Science Center
University of North Texas at Dallas

EXHIBIT 3

October 2022

This Page Intentionally Left Otherwise Blank

1. Introduction

1.1. Executive Summary

The University of North Texas System ("UNT System") Information Security Handbook establishes the information security program framework for the System Administration and Institutions. The UNT System Information Security Handbook contains procedures and standards that support adherence to UNT System Information Security Regulation 6.100. The UNT System is committed to establishing an information security program designed to protect the confidentiality, integrity, and availability of information and information resources. Implementation of an information security program supports business continuity, management of risk, enables compliance, and maximizes the ability of the System Administration and Institutions to meet their goals and objectives. The Information Security Handbook shall comply with federal and state laws related to information and information resources security, including, but not limited to the Texas Administrative Code ("TAC") Title 1 §§ 202 and 203 and the information security framework established in International Standards Organization ("ISO") 27001 and 27002.

1.2. Governance

The UNT System Information Security Handbook is governed by applicable requirements set forth in 1 TAC §§ 202 and 203 and the information security framework established in ISO 27001 and 27002. Refer to 1 TAC §§ 202 and 203 and ISO 27001 and 27002 if a topic is not addressed in the handbook or if additional guidance is needed.

1.3. Scope and Application

The requirements established in the Information Security Handbook apply to all users of information and information resources of the System Administration and Institutions, including students, faculty, staff, guests, contractors, consultants, and vendors.

1.4. Annual Review

As required by 1 TAC § 202.70, a party independent of the information security program shall review the information security program for the System Administration and Institutions. The independent party shall conduct this review annually and revise for suitability, adequacy, relevance, and effectiveness as needed. The Information Security Officer shall coordinate the review. The Chancellor of the System Administration and President of each Institution or their designees shall approve the designation of the independent party.

2. Information Security Definitions

2.1. Definitions

2.1.1. Access. The physical or logical capability to interact with, or otherwise make use of, information and information resources.

2.1.2. Asset. Anything of value to an organization, including information.

2.1.3. Breach. An incident that results in the compromise of confidentiality, integrity, or availability of information or information resources.

2.1.4. Business Continuity Planning. The process of identifying mission-critical information systems and business functions, analyzing the risks and probabilities of service disruptions and outages, and developing procedures to continue operations during outages and restore those systems and functions.

2.1.5. Category I Confidential Information. Information that requires protection from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal agreement, or information that requires a high degree of confidentiality, integrity, or availability.

2.1.6. Category II Proprietary Information. Information that is proprietary to an Institution or has moderate requirements for confidentiality, integrity, or availability.

2.1.7. Category III Public Information. Information with low requirements for confidentiality, integrity, or availability and information intended for public release as described in the Texas Public Information Act.

2.1.8. Change Management. The process responsible for controlling the life cycle of changes made to information resources that are implemented while maintaining the confidentiality, integrity and availability of the information resource.

2.1.9. Cloud Computing Service. A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Service models that represent cloud

computing include Software as a Service (Saas), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing services can be deployed in a private cloud, community cloud, public cloud, or hybrid cloud.

2.1.10. Confidential Information. Information that must be protected from unauthorized disclosure or public release, based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

2.1.11. Configuration Management. A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

2.1.12. Custodian. A person responsible for implementing the Information Owner-defined controls and access to information and information resource. Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by Information Owners for performing tasks, also act as Custodians of the information and are responsible for maintaining the security of the information. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration and Institutions.

2.1.13. Disaster Recovery. The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

2.1.14. Enterprise Information Resource. An information resource that is administered by Information Technology Shared Services ("ITSS").

2.1.15. High Impact Information Resource. An Information Resource whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

2.1.15.1. Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

2.1.15.2. Result in major damage to organizational assets;

2.1.15.3. Result in major financial loss; or

2.1.15.4. Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

2.1.16. Hosting Department. A department contracting with an external party that will require access to institutional information or information resources.

2.1.17. Incident. A security event that results in, or has the potential to result in, a breach of the confidentiality, integrity, or availability of information or an information resource. Security incidents result from accidental or deliberate unauthorized access, loss, disclosure, disruption, or modification of information or information resources.

2.1.18. Information Owner. A person with operational authority for specified information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information.

2.1.19. Information Resources. The procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel including consultants and contractors.

2.1.20. Information Security. The protection of information and information resources from threats in order to ensure business continuity, minimize business risks, enable compliance, and maximize the ability of the System Administration and Institutions to meets their goals and objectives. Information security ensures the confidentiality, integrity, and availability of information and information resources.

2.1.21. Information Security Officer. The Information Security Officer is responsible for developing and administering the operation of an information security program. The Vice Chancellor and Chief Information Officer, or his or her designee, shall appoint an Information Security Officer for the System Administration. The President of each Institution, or his or her designee, shall appoint an Information Security Officer for the Institution. In addition to their administrative supervisors, Information Security Officers will report

to and comply with directives from the Vice Chancellor and Chief Information Officer for all security related matters.

2.1.22. Information Security Program. A collection of controls, policies, procedures, and best practices used to ensure the confidentiality, integrity, and availability of System Administration and Institution owned information and information resources.

2.1.23. Institution. A degree-granting component of the UNT System.

2.1.24. Integrity. The security principle that information and information resources must be protected from unauthorized change or modification.

2.1.25. Least Privilege. The security principle that requires application of the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

2.1.26. Mission Critical. A function, service, or asset vital to the operation of the Institution, which if made unavailable, would result in considerable harm to the Institution and the Institution's ability to fulfill its responsibilities.

2.1.27. Network Devices. Hardware components or software services running on common desktop or information resources that communicate over the institution's network.

2.1.28. Patch. An update to an operating system, application, or other software issued to correct specific problems.

2.1.29. Patch Management. The systematic notification, identification, deployment, installation, and verification of operating system and application software patches.

2.1.30. Penetration Test. A series of activities undertaken to identify and exploit security vulnerabilities.

2.1.31. Personally Identifying Information. Information that alone or in conjunction with other information identifies an individual, including an individual's:

2.1.31.1. Name, social security number, date of birth, or government-issued identification number;

2.1.31.2. Mother's maiden name;

2.1.31.3. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

2.1.31.4. Unique electronic identification number, address, or routing code; and

2.1.31.5. Telecommunication access device as defined by Section 32.51, Penal Code.

2.1.32. Privacy Officer. A person designated by the institution accountable for developing, implementing and maintaining an institution-wide governance and privacy program in accordance with federal and state law.

2.1.33. Privileged Access. An escalated level of resource access that allows changes to information systems and can affect the confidentiality, integrity, or availability of information or information resources. Privileged access is granted to users that are responsible for providing information resource administrative services such as system maintenance, data management, and user support.

2.1.34. Project Leader. The person responsible for the oversight of an information technology projects including an application development or any information resources project.

2.1.35. Recovery Point Objective (RPO). The maximum tolerable period in which data might be lost from an IT service due to a major incident. (i.e., amount of potential data loss).

2.1.36. Recovery Time Objective (RTO). The duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

2.1.37. Removable Media. Any device that electronically stores information and can be easily transported. Examples of removable media include USB flash drives, CD-ROM, DVD-ROM, external or portable hard drives, laptop computers, tablets, or any other portable computing device with storage capabilities.

2.1.38. Risk. The effect on the mission, function, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact.

2.1.39. Risk Assessment. The process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on the System Administration or an Institution's mission, functions, image, reputation, assets, or individuals. Risk assessment incorporates threat and vulnerability analysis and considers mitigations provided by planned or in-place security controls.

2.1.40. Security Exception. An exception granted by the Information Security Officer in response to non-compliance resulting from an inability to meet the requirements of an information security policy, standard, or procedure.

2.1.41. System Administration. The central administrative component of the UNT System.

2.1.42. Transaction Risk Assessment. An evaluation of the security and privacy requirements for an interactive web session providing public access to an institution's information and services.

2.1.43. University of North Texas System. The System Administration and the member Institutions combined to form the UNT System.

2.1.44. User. An individual or automated application authorized to access information or information resources in accordance with the Information Owner-defined controls and access rules.

2.1.45. Vulnerability Assessment. A documented evaluation assessing the extent to which an information resource or data processing conducted by the UNT System Administration or Institutions or by a third-party is vulnerable to unauthorized access or harm, is subject to attack, and the extent to which electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

3. Structure of the Information Security Handbook

The structure of the Information Security Handbook is based on the framework established in ISO 27001 and 27002. In addition, requirements of the handbook are consistent with the Information Security Standards established in 1 TAC §§ 202 and 203, as amended.

3.1. Reference

3.1.1. UNT System Information Security Regulation 6.1000

4. Risk Management and Assessment

4.1. Purpose

All responsible parties must manage risks to information resources. The expense of security safeguards shall be commensurate with the value of the assets being protected and the liability inherent in regulations, laws, contractual obligations, or other agreements governing the assets. Failure to respond to risks could result in accidental or intentional acceptance of institutional risk by an unauthorized individual.

4.2. Requirements

4.2.1. The UNT System Vice Chancellor and Chief Information Officer will commission a system-wide security risk assessment of information resources consistent with UNT System Administration and Institutional compliance and risk assessment plans.

4.2.2. Risk assessments of mission critical and high-risk information resources shall be conducted annually. All information resources shall be assessed biennially.

4.2.3. The risk assessment process must consider the immediate and future impact of a risk to organizational operations.

4.2.4. Risk assessments must use a standard methodology compatible with 1 TAC § 202.75. Identified risks shall be accepted, rejected, mitigated, or transferred using a defined and documented plan.

4.2.5. The Chancellor for System Administration and the President of each Institution or their designated representative is responsible for approving the risk management plan and making risk management decisions based on the risk assessment and either accept exposures or protect the data according to its value and sensitivity.

4.2.6. The Chancellor or President is authorized to make risk management decisions for residual high risks.

4.2.7. The Information Security Officer is authorized to make risk management decisions for residual moderate and low risks.

4.2.8. If a public information request for the risk management plan or a risk assessment is received, the Office of General Counsel for the UNT System shall determine whether the requested information is exempt from disclosure under the Texas Public Information Act.

4.3. Reference

4.3.1. Texas Administrative Code, Title 1 § 202.75; Managing Security Risks
4.3.2. International Standards Organization 27002:2013; Risk Assessment and Treatment
4.3.3. International Standards Organization 27001:2013
4.3.4. National Institute of Standards and Technology 800-30; Guide for Conducting Risk Assessments.
4.3.5. Texas Government Code, Chapter 522; Public Information

5. Information Security Program

5.1. Purpose

The System Administration and Institutions are required to adopt and implement information security programs, policies, and processes consistent with the requirements set out in the Information Security Handbook and shall comply with the requirements of the Information Security Handbook.

5.2. Information Security Program Review

5.2.1. The Information Security Officer will conduct an annual review of the information security program to assess opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.

5.2.2. A workgroup comprised of representatives from the UNT System Administration and each Institution shall review and update the Information Security Handbook annually or as needed. The System Information Security Officer will notify campus Information Security Officers if changes are made to the Information Security Handbook.

5.2.3. The Chief Information Security Officer will review modifications proposed by the handbook workgroup and present to the Vice Chancellor and Chief Information Officer for review and approval

5.2.4. The Vice Chancellor and Chief Information Officer is responsible for approving changes made to the Information Security Handbook.

5.3. Reference

5.3.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head

5.3.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
5.3.3. Texas Administrative Code, Title 1 § 202.74; Institution Information Security Program
5.3.4. International Standards Organization 27002:2013; Organization of Information Security
5.3.5. International Standards Organization 27001:2013

6. Organizational Structure of Information Security

6.1. Purpose

The responsibilities for managing information security are assigned to designated individuals within the organization and external to the organization. Officials of the System Administration and each Institution, as well as external entities, shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1000 and 1 TAC §§ 202.70 - 202.72 and 202.74.

6.2. Internal Organization

The following officials at the System Administration and each Institution shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1000 and 1 TAC §§ 202.70 - 202.72 and 202.74.

6.2.1. System or Institution Head or Designated Representative

The Chancellor for the System Administration and the President of each Institution or their designee is responsible for overseeing the protection of information resources and for reviewing and approving the designation of Information Owners and their associated responsibilities.

6.2.2. Vice Chancellor and Chief Information Officer

The System Vice Chancellor and Chief Information Officer shall be responsible for approval, oversight, and coordination of all information security programs for the System Administration and Institutions.

6.2.3. Information Security Officer

The Chancellor or Vice Chancellor and Chief Information Officer shall appoint an Information Security Officer for the System Administration. The President of each Institution or his or her designee shall appoint an Information Security Officer for the Institution. The Information Security Officer is responsible for developing and administering the operation of an information security program. In addition to their administrative

supervisors, Information Security Officers will report to and comply with directives from the Vice Chancellor and Chief Information Officer for all security related matters.

6.2.4. **Information Owner**

The Information Owner is the person with operational authority for specific information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information. This person shall comply with the requirements of the Information Security Handbook and applicable information security program.

6.2.5. **Custodian**

The Custodian is the person responsible for implementing the Information Owner-defined controls and access to an information resource. Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by Information Owners for performing tasks, also act as Custodians of the information and are responsible for maintaining the security of the information. Custodians may include, but are not limited to, employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration or an Institution.

6.2.6. **User**

A User is an individual or automated application authorized to access an information resource in accordance with the Information Owner-defined controls and access rules.

6.2.7. **Data Management Officer**

Data Management Officer is responsible for ensuring that an institutional data governance program is established, identifying the institution’s data assets, and establishing related process and procedures to oversee the institution's data assets in accordance with state law.

6.3. **External Organization**

6.3.1. The Custodian and Information Owner with cooperation from the hosting department shall manage and review access, permissions, and privileges assigned to vendors, consultants, and other persons of interest to ensure the return of all confidential and proprietary information and information

resource assets and to ensure the removal of computer access when obligations or responsibilities of an external party change.

6.3.2. Written agreements or contracts must be in place between the System Administration or Institution and external party prior to granting access to information or information resources to the external party. The hosting departments shall ensure that security risk assessments and non-disclosure agreements are in place prior to entering into agreements with external parties who will access information resources, Category I Confidential, or Category II Proprietary information.

6.3.3. Custodians shall protect information resources assigned from the System Administration or Institutions to another institution of higher education, or from the System Administration or an Institution to a contractor or other third party in accordance with the policies, standards, and other conditions imposed by the System Administration or Institution.

6.4. Reference

6.4.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
6.4.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
6.4.3. Texas Administrative Code, Title 1 § 202.72; Staff Responsibilities
6.4.4. Texas Administrative Code, Title 1 § 202.74; Institution Information Security Program
6.4.5. International Standards Organization 27002:2013; Organization of Information Security
6.4.6. International Standards Organization 27001:2013

7. Human Resource Security

7.1. Purpose

The System Administration and Institutions must establish rules that describe the responsibilities and expected behaviors of all users of institutional information systems. The System Administration and Institutions shall update rules regularly according to security and institutional policy changes. All employees and contractors must understand their roles and responsibilities pertaining to information security. Supervisors and Information Owners are responsible for reviewing and modifying employee access to information and information resources. Information Owners and university officials that are responsible for hosting contractors are also responsible for reviewing and modifying access to information and information resources when changes occur in employment status or written agreements.

7.2. **Access Agreements**

Access agreements must be established prior to granting employee and contractor access to institutional information and information resources.

7.2.1. Access agreements shall include a signed acknowledgment that the user understands responsibilities and expected behaviors of accessing institutional information resources.

7.2.2. Access agreements must be reviewed, modified, and acknowledged as changes are made to user responsibilities and expected behaviors.

7.2.3. Access agreements must be reviewed, modified, and acknowledged in the event of employment status changes, terminations, or changes in written agreements.

7.3. **Prior to Employment and Delivery of Services**

7.3.1. The System Administration and Institutions must ensure that employees and contractors receive cybersecurity awareness training and must inform employees and contractors about security policies and procedures during the onboarding process and prior to granting access to information resources.

7.3.2. Employees and contractors must complete cybersecurity awareness training during orientation or onboarding.

7.4. **During Employment and Delivery of Services**

7.4.1. Employees and contractors must complete annual certified cybersecurity awareness training. Supervisors shall ensure that employees participate in training for the handling of sensitive and confidential data as appropriate for their role. Employees must also complete training that is commensurate with their responsibilities and job duties, including but not limited to continuing education.

7.4.2. Employees and supervisors must document and monitor completion of security training and retain employee training records as required by retention schedules.

7.5. **Termination, Changes of Employment, and Cessation of Services**

The System Administration and Institutions must have exit procedures in place to ensure the return of all confidential and proprietary information and information resource assets upon termination of employment, cessation of services, or cessation

written agreements and ensure the timely removal of computer access when the employment status, contractual obligation, or responsibilities of an individual changes.

7.5.1. Responsibilities and duties that change or remain valid after termination should be contained in a written agreement or contract between the employee and the System Administration or Institution.

7.5.2. The terminating employee's immediate supervisor and a contractor's hosting department are responsible for managing security aspects of the termination, including the return of information and information resource assets, the removal of access rights, and providing notification to information owners of the change in access.

7.5.3. An employee's former and new supervisors should manage changes in responsibilities of employment as roles are terminated and new roles initiated. Former supervisors should review roles, privileges, and physical access to ensure that access no longer needed is disabled. New supervisors should review roles, privileges, and physical access to ensure that access needed for new job responsibilities is granted in accordance with Least Privilege and as appropriate for the sensitivity of the position.

7.5.4. The immediate supervisor of an employee, whose employment status changes, shall notify the Information Owners and custodians of information resources about the change as soon as possible.

7.6. Reference

7.6.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
7.6.2. International Standards Organization 27002:2013; Human Resources Security
7.6.3. International Standards Organization 27001:2013
7.6.4. Payment Card Industry Data Security Standards 3.0

8. Asset Management

8.1. Purpose

The System Administration and Institutions must develop policies and procedures for managing information and information resource assets and should maintain a documented inventory of institutionally owned physical assets and software assets associated with information processing. Information and information resource assets must be identified, classified, documented, prioritized according to criticality,

have documented owners, have documented custodians, be assessed for risk and be managed through the system development life cycle. Policies and procedures ensure the security of information resource assets against unauthorized or accidental modification, destruction, or disclosure. These controls are to ensure the confidentiality, integrity, and availability of information and other assigned information resources.

8.2. **Responsibility for Information and Information Resource Assets**

8.2.1. The System Administration and Institutions shall identify owners, custodians, and users of information and information resource assets and document their responsibilities.

8.2.2. Information Owners must maintain inventories of vendors or third parties that access or process institutional information.

8.2.3. Custodians and Information Owners must conduct and maintain inventories of information resources that collect, use, maintain, and/or share confidential information or personally identifying information.

8.2.4. Custodians that manage, use, and/or store confidential information must develop an inventory of data that documents data flow mapping, how data are transmitted, and storage locations of confidential data.

8.2.5. Custodians of information resources that manage, use, and/or store confidential information must maintain inventories of critical information system components.

8.3. **Information Classification and Handling**

8.3.1. Categories of Information

The Information Owners and Custodians, in coordination with the Information Security Officer, must inventory and classify information. The System Administration and Institutions shall use the following information classification system to categorize information for risk assessments, making risk management decisions, establishing controls, and for protecting information:

8.3.1.1. Category I includes confidential information that all users of information resources must protect from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal

agreements, or information that requires a high degree of confidentiality, integrity, or availability. Owners and Custodians of information resources must label and protect Category I Confidential Information. Confidential information must not be released or made available or accessible to unauthorized individuals.

8.3.1.2. Category II includes information that is proprietary to an institution or has moderate requirements for confidentiality, integrity, or availability. Proprietary Information may not be released without approval from the Office of General Counsel.

8.3.1.3. Category III includes public information with low requirements for confidentiality, integrity, or availability and information intended for public release as described in the Texas Public Information Act. Public information may not be released without approval from the Office of General Counsel.

8.3.2. Information Owners are responsible for identifying information, supporting inventories of information, and classifying information under their authority with the established information security classification categories.

8.3.3. Custodians are responsible for conducting inventories of information systems and technology for which they manage, administer, or for which they have been assigned custody.

8.3.4. The Information Security Officer is responsible for reviewing the institution's inventory of information systems and related ownership and security responsibilities.

8.3.5. Custodians and Project Leaders are responsible for ensuring that data are protected in accordance with data classification identified in this Handbook upon initiation of an information resource technology project.

8.4. **Information Safeguards**

8.4.1. Custodians of information resources, including external parties providing outsourced information resource services, must implement physical, technical, and procedural safeguards for information resources that are commensurate to the criticality of the information system and classification of data used or processed in the information resource or services.

8.4.2. The System Administration and Institutions must dispose of electronic records and devices according to institutional record retention policies and by employing sanitization methods with the strength and integrity in proportion to the security classification and confidentiality of information.

8.4.3. Owners and Custodians of information resources shall label Category I confidential information in physical and electronic formats except in cases where the asset is encrypted.

8.4.4. The Information Security Officer or delegates must review new computer applications and services that receive, maintain, and/or share confidential data to ensure compliance with data security requirements.

8.4.5. Prior to the purchase of information technology hardware, software, and systems development services for any new services, a department must consult with the Information Security Officer or delegates to identify security requirements and develop risk mitigation plans.

8.4.6. The System Administration or Institution is responsible for ensuring that obligations for adhering to information security requirements are included in contracts and other written agreements with vendors. Vendors are required to adhere to identified information security requirements.

8.4.7. Custodians must establish and enforce the principle of Least Privilege when developing standards, procedures, or assigning access permissions.

8.4.8. Information systems accessible to the public should not store or process Category I confidential or Category II proprietary information.

8.4.9. Custodians that administer websites should review information posted to publicly accessible systems at least annually to ensure neither Category I confidential nor Category II proprietary information is included.

8.4.10. Users may view Category III public information on public websites or other publicly available information systems without authentication or identification.

8.4.11. Custodians must consult with the Information Security Officer or delegates to assess new computer applications, systems, and services that support critical business operation or process category I confidential information for vulnerabilities prior to their implementation and throughout the systems lifecycle.

8.4.12. Upon the initiation of any information resource technology project or application development, the System Administration and Institutions shall:

8.4.12.1. Classify any institutional data created or used in the project;

8.4.12.2. Determine and assign the appropriate security controls for the data;

8.4.12.3. Determine the retention requirement for each classification.

8.4.13. Users should minimize the use of personally identifying information and confidential data and use this protected information only when needed in order to meet stated business objectives. Where not needed, users should not collect, store, use or process Personally Identifiable Information or confidential data. Users must protect personally identifying information and confidential data in accordance with this Handbook and conduct a risk assessment prior to use to establish appropriate controls that protect personally identifying information and confidential data.

8.4.14. Use of Personally Identifiable Information or confidential data during testing, training, and research purposes must be minimized to only that which is needed in order to meet stated objectives. The quantity of personally identifying information or confidential data collected, stored or processed should be limited to samples that are needed to validate stated purpose during testing, training, and when conducting research.

8.5. **Systems Currency**

8.5.1. To ensure that the delivery of reliable, low risk, cost effective services, the System Administration and Institutions will reduce and, where possible, eliminate instances of unsupported software and systems.

8.5.2. Custodians should include software replacement schedules in their technology planning before the software is no longer supported by the vendor or manufacturer.

8.5.3. In compliance with 1 TAC 202, the System Administration and Institutions will conduct a high-level risk assessment of software currency and either request necessary upgrades or replacement costs in their budget request, or determine the risk is tolerable based on system data, infrastructure, and vulnerability and business requirements. Risk decisions must be documented and approved by university leadership that is responsible for

overseeing the business functions that are supported by the system or technology that is not current.

8.6. **Reference**

8.6.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
8.6.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
8.6.3. Texas Administrative Code, Title 1 § 202.72; Staff Responsibilities
8.6.4. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
8.6.5. International Standards Organization 27002:2013; Asset Management
8.6.6. International Standards Organization 27001:2013
8.6.7. Texas Government Code 2054.

9. Access Control

9.1. **Purpose**

The System Administration and Institutions shall establish policies and procedures to ensure that no single person can access, modify, or use assets without authorization or detection.

9.2. **User Access Management**

9.2.1. The System Administration and Institutions shall ensure user access is managed with established procedures related to account creation, monitoring, control, and removal, including but not limited to authorization, approval for access by data owners, acknowledgment of user responsibilities, managing passwords, periodic access reviews, and prompt removal of access during role change or termination.

9.2.2. Information Owners and Custodians shall restrict user access, including privileged access, to information and information resources according to the principle of Least Privilege.

9.2.3. User behavior, activities, or the use of computing devices to access institutional networks must not compromise the security of users, information, or information resources.

9.2.4. Institutional or external networks must not be used to compromise the identity of or impersonate individuals or information resources.

9.2.5. Privileged access to information resources is intended to be granted to custodians of information resources and not to end-users. Privileged access shall only be granted as required by business need or job duties.

9.2.6. Information Owners or their delegates and Custodians, shall grant and maintain privileged user access in accordance with the UNT System Information Ownership Guide.

9.2.7. Unless explicitly authorized by the Information Owners or their delegates, Custodians must not grant privileged access to information resources.

9.2.8. The duration of privileged access shall not last longer than needed to perform functional job duties.

9.2.9. Custodians will assign privileged access rights to a different user ID than those used for regular day-to-day activities.

9.2.10. Individuals with privileged access rights must have the appropriate skills and knowledge to securely administer technology and maintain the confidentiality, integrity, and availability of the information resources for which they are granted access. Individuals with privileged access rights must keep their skills and knowledge current to maintain privileged access.

9.2.11. Requests for privileged access will be declined if appropriate administrator or technical skills and knowledge are not attained that are commensurate with the criticality of a system or the protection requirements of data processed or stored in an information system or application.

9.2.12. Privileged access may be revoked in the event of a violation of security policy, procedure, or mandate.

9.2.13. Custodians should avoid the use of default privileged accounts. If using default privileged accounts cannot be avoided, Custodians must employ compensating controls to ensure the security of the information resource.

9.2.14. Information Owners must review access rights in accordance with the UNT System Information Ownership Guide.

9.3. Password Standards

Passwords are a critical control used to control access and protect the confidentiality, integrity, and availability of institutionally owned information and information resources.

9.3.1. Passwords must meet or exceed the following standards for all systems owned or managed by UNT System and Component Institutions:

9.3.1.1. Passwords must have a minimum length of 8 characters;

9.3.1.2. Passwords have a maximum length of 30 characters;

9.3.1.3. Password complexity must include uppercase letters, lowercase letters, and digits;

9.3.1.4. Spaces and backslash are prohibited characters; and

9.3.1.5. The use of common dictionary words is prohibited.

9.3.2. Credentials used for UNT System or Institution owned information resources must not be reused on other systems or services.

9.3.3. Users must change passwords at least annually. The password expiration period may be shorter for some systems based on business or compliance needs.

9.3.4. The use of shared or generic privileged accounts, such as Administrator or root, should be avoided if possible. These accounts should only be used for maintenance, system repair, or recovery operations. They should not be used for day-to-day operation.

9.3.4.1. Custodians should change the credentials for any system or generic account from the default value supplied by the vendor before the system is placed in a production capacity or is put on a public network.

9.3.4.2. Custodians must escrow credentials with their supervisors and backup personnel for generic privileged accounts for systems critical to business operations.

9.3.4.3. Custodians must change passwords for shared or generic privileged accounts when an employee with access to the credentials leaves the organization or changes roles within the organization. This should be done before the employment change occurs if possible, to ensure the confidentiality, integrity, and availability of the information resource tied to the credentials.

9.3.5. Administrative, privileged, and service account password composition and complexity that does not meet these requirements must have mitigating controls approved by the Information Security Officer.

9.3.6. The Information Security Officer may grant an exception if a system is unable to accommodate these requirements.

9.4. User Responsibilities

9.4.1. Users are responsible for all activities related to their accounts.

9.4.2. Users must keep their accounts and passwords secure.

9.4.3. Passwords must not be shared with anyone and are considered Category I confidential information.

9.4.4. Passwords must be protected during automatic log on sessions.

9.4.5. Users must adhere to Section 9.3, Password Standards.

9.4.6. Users should only access information and use information resources that are required to perform job duties.

9.5. Operating System Access Control

The System Administration and Institutions shall develop policies and procedures that govern access to operating systems of institutionally owned computing devices and servers.

9.5.1. Custodians should control access to operating systems by a secure log on procedure.

9.5.2. All user accounts should have a unique identifier to trace activities to the responsible individual.

9.5.3. Custodians are responsible for ensuring that logon banners are presented to users during the log on process that specify user rights and responsibilities regarding system usage.

9.5.4. Custodians are responsible for adhering to section 9.2, User Access Management, in regard to limiting use of administrator and privileged access. Individuals must have a documented business reason for being granted the access.

9.5.5. Users may not employ tools or utilities capable of overriding system and application controls without permission from Custodians.

9.5.6. Administrator accounts or accounts with expanded privileges should only be used for administration and management of information resources.

9.5.7. Shared administrator accounts or accounts with expanded privileges will only be granted based on a documented business need. Custodians must

implement controls to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

9.5.8. Custodians must verify the identity of a user prior to the activation of an administrator account or an account with expanded privileges.

9.5.9. End-Users are not authorized to hold privileged or administrative user roles within information systems.

9.5.10. Individuals that are authorized to use shared administrator accounts or accounts with expanded privileges must agree to keep authentication information confidential and maintained solely within the group authorized to use the privileged account. Authentication information must change if group membership changes.

9.5.11. Custodians must change default vendor authentication information following installation of systems or software.

9.5.12. Individuals that hold administrator accounts or accounts with expanded privileges must adhere to the System Administrator Code of Ethics as referenced in Appendix A of this document.

9.5.13. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in Section 9.3, Password Standards.

9.5.14. Custodians must review authorizations for privileged access rights at regular intervals and must document changes to privileged accounts.

9.5.15. Custodians should define and impose time parameters for session termination.

9.6. Application Access Control

9.6.1. Use of applications is restricted to use terms as described in contract agreements.

9.6.2. Custodians should track licenses for applications that are limited by quantity in order to control unauthorized copying and distribution, as applicable.

9.6.3. Information System Owners must control and document use of peer-to-peer file sharing technology to prevent unauthorized distribution or reproduction of copyrighted work.

9.6.4. Users may not employ tools or utilities capable of overriding application controls.

9.6.5. Custodians should log or document access to mission critical applications.

9.6.6. Shared administrator accounts or accounts with expanded privileges will only be granted based on a documented business need. Custodians must implement controls to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

9.6.7. Custodians must verify the identity of a user prior to the activation of an administrator account or an account with expanded privileges.

9.6.8. Users authorized for shared administrator accounts or accounts with expanded privileges must agree to keep authentication information confidential and maintained solely within the group authorized to use the privileged account. Authentication information must change if group membership changes.

9.6.9. Custodians must change default vendor authentication information following installation of systems or software.

9.6.10. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in Section 9.3, Password Standards.

9.6.11. Custodians must review authorizations for privileged access rights at regular intervals and must document changes to privileged accounts.

9.6.12. Custodians should define and impose time parameters for session termination.

9.6.13. Custodians should authorize access through internal connections by resource type and documented according to the interface characteristics, security requirements, and information classification.

9.7. **Information Access Control**

9.7.1. Information Owners and Custodians should restrict access to data according to the principle of Least Privilege.

9.7.2. Information Owners and Custodians should log or document access to Category I confidential information.

9.7.3. Custodians shall authorize access to information through internal connections by resource type and documented according to the interface characteristics, security requirements, and information classification.

9.8. Mobile Computing and Teleworking

9.8.1. Users must follow security policies and procedures and adhere to the requirements of this Handbook when using or accessing institutional information and information resources remotely.

9.9. Reference

9.9.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
9.9.2. International Standards Organization 27002:2013; Access Control
9.9.3. International Standards Organization 27001:2013
9.9.4. System Administrator Code of Ethics
9.9.5. UNT System Information Ownership Guide

10. Cryptographic Controls

10.1. Purpose

The System Administration and Institutions must develop policies and procedures implementing encryption requirements for information storage devices, data transmission, portable devices, removable media, and encryption key standards based upon the requirements established by the institution providing the service.

10.2. Requirements

10.2.1. The System Administration and Institutions must encrypt institutionally owned mobile devices. If a device is not capable of encryption, no Category I confidential data may be stored on the device.

10.2.2. Minimum encryption requirements must include the following:

10.2.2.1. Custodians must encrypt confidential information transmitted over a public network;

10.2.2.2. Custodians must encrypt confidential information that is stored in a public location that is directly accessible without compensating controls;

10.2.2.3. All users must encrypt confidential information if copied to

or stored on a portable computing device, removable media, or non-agency owned computing device;

10.2.2.4. Custodians must implement compensating electronic controls to secure a device that cannot be encrypted. Compensating controls must be approved by the information security officer.

10.2.2.5. IT Managers must be able to document and verify the encryption of a device.

10.2.2.6. Administrators of key management systems are responsible for ensuring that encryption keys are securely managed.

11. Physical and Environmental Security

11.1. Purpose

Implementation of physical security measures help to protect information and information resources from unauthorized access. Physical security is a critical aspect of information security.

11.2. Secure Areas

11.2.1. The System Administration and Institutions must document and manage physical security for mission critical information resources to ensure confidentiality, integrity, and availability of information resources; including maintaining records concerning the entrance and exit times of onsite visitors. Custodians that are responsible for secure areas should maintain access records in accordance with institutional retention policies.

11.2.2. The administrator of an information processing facility must ensure that the facility is protected with physical controls that are appropriate for the size and complexity of the operations, requirements concerning criticality, sensitivity, and regulatory compliance requirements, and risks to the systems or services operated at those locations.

11.2.3. The administrator of work areas within an information processing facility must protect work areas within the facility in accordance with physical controls and security requirements that are appropriate for the type of operational functions performed in the area. The System Administration and Institutions shall develop procedures that distinguish between the responsibilities of onsite personnel and visitors in sensitive areas.

11.2.4. The administrator of a facility or work area must document, test, and review physical security and emergency procedures for information resources as part of the risk assessment process.

11.2.5. On-site personnel shall only be granted access to information processing facilities in accordance with job responsibilities.

11.2.6. The administrator of a secure area shall limit knowledge of the existence of, or activities within, the secure area based on a need-to-know.

11.2.7. Supervisors must monitor personnel working in secure areas. The level of supervision should be appropriate for the type of operational function performed in the area, adhere to the relevant regulatory compliance requirements, and consider identified applicable risks.

11.2.8. The administrator of a secure area is responsible for ensuring that the area is locked, or otherwise secured, and periodically inspected.

11.2.9. The use of equipment to photograph, record video, and/or record audio is prohibited in secure areas unless explicitly authorized by the administrator of the secure area.

11.3. **Equipment Security**

11.3.1. Custodians must document, update, and test at least annually, procedures protecting mission critical information resources from environmental hazards, power failures, and other disruptions.

11.3.2. Administrators of secure areas shall ensure that employees that work in the area or provide support within the area are trained to monitor environmental controls, have knowledge of environmental control procedures and equipment, and are aware of response protocols for emergencies or equipment problems.

11.3.3. Office areas and computer screens should remain clear of Category I confidential information when a device or office is unattended.

11.3.4. Category I confidential information should never be left unattended on media such as printers, fax machines, and other devices.

11.3.5. All users should lock away Category I confidential information that is in print format or stored on portable media when not in use or when an office is vacant. Physical media includes, but is not limited to computers, removable storage devices, and printed information.

11.3.6. All users should log off or protect unattended computers with a screen and keyboard locking mechanism controlled by a password, token, or similar authentication mechanism.

11.3.7. Use of photocopiers, scanners, digital cameras, and other reproduction technology for unauthorized duplication of Category I confidential data is prohibited.

11.4. **Equipment Maintenance**

11.4.1. Custodians must maintain equipment in accordance with the vendor's recommended service intervals and specifications.

11.4.2. Only authorized maintenance personnel should carry out repairs or service equipment.

11.4.3. Records should be kept of all preventative and corrective equipment maintenance.

11.4.4. Records should be kept of all suspected or actual equipment errors.

11.4.5. Custodians should implement controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel onsite or external to the organization. Where necessary, custodians should clear confidential information from the equipment, or ensure the maintenance personnel have appropriate authorization.

11.4.6. Custodians should follow vendor or service provider maintenance recommendations pending the existence of operational or risk management considerations. Compensating controls or security exceptions must exist if vendor or service provider maintenance recommendations cannot be followed.

11.4.7. Custodians must inspect and test equipment prior to placing in operation to ensure integrity and proper function and to verify that all potentially impacted security controls are intact.

11.4.8. Custodians must monitor and approve maintenance activities and ensure that explicit approval is obtained prior to removing equipment.

11.5. **Reference**

11.5.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

11.5.2. International Standards Organization 27002:2013; Physical and Environmental Security

11.5.3. International Standards Organization 27001:2013

12. Operations Security

12.1. Purpose

Custodians must implement documented operating procedures to protect data, minimize interruption to business activities, and ensure the integrity and availability of information.

12.2. Operational Procedures and Responsibilities

12.2.1. Custodians of critical services and systems must develop and annually update a security plan for those services.

12.2.2. Custodians must establish and enforce the principle of Least Privilege when developing standards, procedures, or assigning access permissions.

12.2.3. Custodians must establish a separation of functions for tasks involving information and information resources that are susceptible to fraudulent or other unauthorized activity.

12.2.4. The System Administration and Institutions must follow password policies and procedures, established by the System Administration or Institution, that provide the password management service and are also consistent with ISO 27002 and the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

12.2.5. The System Administration and Institutions must follow policies and procedures that govern access, management, and monitoring of communication networks and devices that are established by the System Administration or Institution providing communications service consistent with ISO 27002 and the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

12.2.6. The System Administration and Institutions must implement controls to protect information and information resources from malicious or unauthorized code. The System Administration or Institution providing the service is responsible for establishing standards for management of anti-virus protection.

12.2.7. The System Administration and Institutions must create procedures for the use of digital signatures that comply with provisions found in 1 TAC § 203.

12.2.8. The System Administration and Institutions must implement system identification/logon banners, which have warning statements that indicate the system is the property of the System Administration or an Institution. The identification/logon banner shall include the following topics at minimum:

12.2.8.1. Unauthorized use is prohibited;

12.2.8.2. Usage may be subject to security testing and monitoring;

12.2.8.3. Misuse is subject to penalties and/or criminal prosecution; and

12.2.8.4. Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

12.2.8.5. By using or accessing a university information resource you consent to allowing the institution to collect identifiable information that includes unique electronic identification numbers, routing codes, network address, internet protocol address, and other information that is collected from your browser, device, or information that is provided by you during your use of the information resource.

12.3. **Protection against Malware, Malicious, or Unwanted Programs**

The System Administration and Institutions shall establish policies and procedures regarding malware, malicious, or unwanted programs. Policies and procedures should address malware on system, application, and network layers.

12.3.1. Custodians must install centrally administered antivirus software on all computing information resources managed by System Administration or Institutions.

12.3.2. Custodians must keep antivirus software current.

12.3.3. IT Managers must configure antivirus software so that users cannot disable or prevent the software from functioning properly.

12.3.4. The Information Security Officer shall ensure that automated tools are available to scan information resources for malware, malicious programs, or unwanted programs.

12.3.5. Information resources owned by the System Administration and its Institutions must meet the following standards:

12.3.5.1. Communicate with the security management server every 120 days;

12.3.5.2. Have antivirus definitions installed that are no more than seven days old; and

12.3.5.3. Run supported versions of the antivirus software, security management server, and antivirus engine.

12.3.6. IT Managers are responsible for providing the following support to computing devices:

12.3.6.1. Installing current versions of antivirus and encryption software on all newly acquired laptops prior to deployment;

12.3.6.2. Ensuring laptop computers receive updates and patches;

12.3.6.3. Investigating laptop computers that do not meet the standards established in 12.3.3. of this standard and documenting any variances from compliance;

12.3.6.4. Resolving variances from compliance that fall within their support responsibilities; and

12.3.6.5. Removing laptop computers from security management server when decommissioned or no longer in use.

12.3.7. The custodial department must submit a request for a security exception if they cannot meet the requirements of this Handbook. Security exception requests must be submitted to the Information Security Officer and include the following:

12.3.7.1. The custodial department name, location, and contact.

12.3.7.2. The service and asset tag numbers of the laptop computer.

12.3.7.3. Location of the laptop computer.

12.3.7.4. Current use of the laptop computer.

12.3.7.5. Reason why the variance cannot be resolved.

12.3.7.6. Reason why the laptop computer cannot be decommissioned.

12.3.7.7. Compensating controls that may mitigate the risk of non-compliance.

12.3.7.8. Supplemental documentation that may exist in support of the request.

12.4. Back-Up

The System Administration and Institutions are required to regularly backup and test mission critical information. Backup processes shall be defined to protect the confidentially, integrity, and availability of the stored information.

12.5. Media Handling

The System Administration and Institutions must implement policies and procedures regarding the secure management of removable media. Policies should address encryption, storage, transport, and the secure destruction of any data commensurate with the value and sensitivity of the information.

12.5.1. All users must protect physical media containing Category I confidential information in accordance with the requirements established herein and as required in applicable laws, regulations or standards. The Information Owner must approve user access rights and authorizations for copying of data.

12.5.2. Custodians must maintain strict protection controls over media containing Category I confidential information. Custodians must track the chain of custody if the media is transported beyond its original location and transferred to another Custodian.

12.5.3. Protections should include using reliable couriers that are bonded and insured, maintaining chain of custody by keeping accurate logs of the content of the media, the protection applied, times of transfer to the alternate location, receipt at the destination and appropriately protecting media during transit.

12.5.4. Custodians must ensure that USB drives are configured to protect confidential information. USB drives must be prevented from storing data except in situations where administration of a device warrants use of the drive, and in cases where a user has obtained a security exception to store

encrypted data on the drive. Data loss prevention software, encryption, and blocking drives on mount, are acceptable solutions for protecting USB drives.

12.6. **Electronic Commerce**

The System Administration and Institutions shall define security protections, where applicable, to secure online transactions for electronic commerce. Processing and acceptance of payment card transactions must follow the Payment Card Industry Data Security Standards ("PCI DSS") as appropriate. Third-party processors must also demonstrate compliance with PCI DSS.

12.7. **Monitoring**

12.7.1. Custodians must establish security monitoring and logging practices. Monitoring activities should include procedures for contacting Information Security to report activities that indicate a security incident has occurred. Custodians should retain logs in accordance with operational and compliance needs. Custodians should ensure logs include histories of transactions that capture system and user authentication and must comply with the requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC 202.76.

12.7.1.1. Monitoring and logging functions must provide audit trails to ensure accountability for updates to mission critical information, hardware, and software.

12.7.1.2. Custodians for enterprise systems should produce, maintain, and regularly review event logs that record user activities, exceptions, faults, and information security events.

12.7.2. Custodians must establish controls to ensure the confidentiality and integrity of information in system logs, transaction histories, and other system audit information. Custodial departments must monitor and store access to this information in a location that is separate from the systems generating the information.

12.7.3. The organization must retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

12.8. **Internet Website and Mobile Applications**

12.8.1. Websites and mobile applications must meet security requirements identified in the Handbook, including by not limited to Sections 9. Access Control and 14. Information System Acquisition, Development, Testing, and Maintenance, prior to being placed into production.

12.8.2. The developer of a website or mobile application that processes confidential information must submit the information listed below to the information security officer for assessment:

12.8.2.1. A description of the website or application architecture,

12.8.2.2. The authentication mechanism for the website or application,

12.8.2.3. The administrator-level access to data included in the website or application, and

12.8.2.4. A security plan to establish planned beta testing of the website or mobile application.

12.8.3. The developer or entity acquiring a website or mobile application that processes sensitive personal information, personally identifying or confidential information must subject the website and mobile application to vulnerability and penetration testing before deployment or acquisition and address any vulnerability identified before deployment or acquisition.

12.9. **Reference**

12.9.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
12.9.2. Texas Administrative Code, Title 1, Chapter 203; Management of Electronic Transactions and Signed Records
12.9.3. International Standards Organization 27002:2013; Communications and Operations Management
12.9.4. International Standards Organization 27001:2013

13. Communications Security

13.1. **Purpose**

The System Administrations and Institutions must develop policies and procedures to protect institutional data, minimize interruption to business activities, and ensure the integrity and availability of information.

13.2. **Network Security Management**

13.2.1. The System Administration and Institutions should develop policies and procedures for the secure management, access, monitoring, and control of institutionally owned and managed communications networks. Policies or procedures should require the following:

13.2.1.1. Information System Owners must restrict access to the network to authorized devices and users. Owners must log or otherwise document network access;

13.2.1.2. Network access must adhere to the principle of Least Privilege;

13.2.1.3. Information System Owners must develop and communicate secure remote access procedures;

13.2.1.4. Networks must be segmented by function;

13.2.1.5. Information System Owners must implement appropriate security controls based on the criticality and value of the resources on the network;

13.2.1.6. Networks must be monitored; and

13.2.1.7. Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided internally or outsourced.

13.2.2. Network Connections

13.2.2.1. Only authorized network devices may connect to university networks. The introduction of network devices or information resources that negatively affect the behavior or security of the network or violate university policies, are prohibited.

13.2.2.2. The Chief Technology Officer must approve the addition of network devices that could conflict with other approved devices on the network, alter the institution's network topology, or place high demands on network bandwidth prior to their introduction for UNT system, UNT Dallas, and UNT.
The Chief Information Officer of HSC, or designee, must approve the addition of network devices that could conflict

with other approved devices on the network, alter the institution's network topology, or place high demands on network bandwidth prior to their introduction for HSC. The following examples of types of devices require approval:

13.2.2.2.1. Multicasting;

13.2.2.2.2. Services that answer broadcast messages, such as DHCP and BOOTP;

13.2.2.2.3. Devices that answer ARP requests as servers (such as security tools and network management tools);

13.2.2.2.4. Firewalls that operate at a level higher than a single machine in the network hierarchy;

13.2.2.2.5. Routers;

13.2.2.2.6. Bridges;

13.2.2.2.7. Switches;

13.2.2.2.8. Proxy servers;

13.2.2.2.9. Wireless access points;

13.2.2.2.10. High bandwidth devices; and

13.2.2.2.11. Other similar devices.

13.2.2.3. If a device on the network is found to compromise any aspect of the network's operation, IT Shared Services in coordination with the local IT support, may remove the device from the network.

13.3. **Information Transfer**

13.3.1. The System Administration and Institutions must implement policies and procedures ensuring that the transfer of information within and external to the organization is secure.

13.3.2. Custodians must protect information exchanged with an external institution, agency, or organization as required by the System Administration or

Institution policies in accordance with the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

13.3.3. Custodians should establish controls to ensure confidential information leaving UNT System is protected with encryption.

13.3.4. Information transfer agreements must govern the transfer of information to an external institution, agency, or organization to ensure the confidentiality and integrity of institutionally owned data. Information transfer agreements should include the following:

13.3.4.1. Management responsibilities for controlling and notifying transmission dispatch and receipt;

13.3.4.2. Procedures to ensure traceability and non-repudiation;

13.3.4.3. Minimum technical standards for packaging and transmission;

13.3.4.4. Escrow agreements;

13.3.4.5. Courier identification standards;

13.3.4.6. Responsibilities and liabilities in the event of information security incidents, such as loss of data;

13.3.4.7. Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected;

13.3.4.8. Technical standards for recording and reading information and software;

13.3.4.9. Any special controls that are required to protect sensitive items, such as cryptography;

13.3.4.10. Maintaining a chain of custody for information while in transit; and

13.3.4.11. Acceptable levels of access control.

13.4. **Reference**

13.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
13.4.2. Texas Administrative Code, Title 1, Chapter 203; Management of Electronic Transactions and Signed Records
13.4.3. International Standards Organization 27002:2013; Communications and Operations Management
13.4.4. International Standards Organization 27001:2013

14. Information System Acquisition, Development, Testing, and Maintenance

14.1. Purpose

Information System Owners should identify security requirements and include the requirements in development, acquisition, testing, maintenance, and implementation of information resources.

14.2. Security Requirements of Information Systems

14.2.1. Information System Owners must consider security and compliance requirements in all phases of computer system or software development lifecycles and the systems acquisition process.

14.2.2. The System Administration and Institutions must implement change and configuration management processes for controlling modifications to hardware, software, firmware, and documentation. Custodians must document and implement baseline configurations for all network devices and information systems. Custodians must use the established change control and configuration management procedures for the review and approval of changes to baseline configurations to ensure compliance.

14.2.3. Custodians must implement change management procedures that include security impact analysis, risk assessment with likelihood of success, significance to business resources required, business justification, testing changes prior to deployment, change deployment plan, guidance for change prioritization, and communication to affected users, prior to deployment of changes. Custodians must consider change management in project management practices.

14.2.4. For each change, Custodians must perform and retain evidence of pre-deployment and post-deployment testing to ensure the appropriate level of testing is performed and signoffs are provided by business and/or IT stakeholders

14.2.5. Custodians must implement the requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, when testing data or managing test, development, and quality assurance environments.

14.2.6. Custodians must design and configure information resources to protect personally identifying information and confidential data.

14.2.7. Custodians must ensure that multi-user information systems are assessed by the Information Security Officer to ensure compliance with security policies and to ensure that appropriate controls are in place prior to placing the information system into production and before configuration or other changes occur.

14.2.8. Custodians of information resources must manage information resources in a manner that ensures that updates and patch management practices ensure compliance with vendor's recommended update and patch intervals, as indicated in best practice, or provide comparable compensating controls that mitigate risk resulting from out-of-date software. Patch management implementation must include:

14.2.8.1. Prioritization of patches and system updates;

14.2.8.2. Specification that patches are to be applied at regular intervals;

14.2.8.3. Aligned maintenance windows with vendor patch and update release schedules;

14.2.8.4. Patch monitoring for correct installation;

14.2.8.5. Problems shall be addressed as they occur; and

14.2.8.6. Contingency plans for handling emergency or critical updates.

14.2.8.7. End-of-life procedures to address older systems using one or more of the following approaches:

14.2.8.7.1. Decommission system

14.2.8.7.2. Upgrade to latest platform

14.2.8.7.3. Migrate to another platform

14.2.8.7.4. Manage risk through use of compensating controls

14.2.8.8. Custodians must request a security exception from the Information Security Officer for systems that have reached end-of-life.

14.2.9. Custodians must protect documents, procedures, and guidelines associated with administration or implementation of information systems from unauthorized disclosure that include:

14.2.9.1. Secure configuration, installation, and standard operating procedures;

14.2.9.2. Effective use and maintenance of security functions;

14.2.9.3. Known vulnerabilities regarding configuration and use of administrative functions;

14.2.10. The System Administration and Institutions must implement policies and procedures that ensure development of continuous monitoring of information system security controls.

14.3. Correct Processing in Applications

14.3.1. The System Administration and Institutions must develop and implement procedures to ensure the confidentiality, integrity, and availability of information if the institution engages in software engineering or development.

14.4. Security in Development and Support Processes

Custodians must consider information security in all phases of the system development lifecycle or acquisition process.

14.4.1. The System Administration and Institutions should establish standards for the secure development of software, systems, and architecture and consider the following:

14.4.1.1. Security of the development environment;

14.4.1.2. Security in the software development methodology;

14.4.1.3. Secure coding guidelines for each programming language used;

14.4.1.4. Security requirements in the design phase;

14.4.1.5. Security checkpoints within the project milestones;

14.4.1.6. Secure repositories;

14.4.1.7. Security in version control;

14.4.1.8. Required application security knowledge;

14.4.1.9. Developers' capability of avoiding, finding, and remediating vulnerabilities; and

14.4.1.10. Planning for addressing end of support by the vendor.

14.4.2. Custodians are responsible for maintaining the security of systems and keeping software up to date.

14.4.3. Custodians are responsible for developing security plans for information resources that they manage prior to deployment. Security plans should include consideration of networks, facilities, systems, and other information resources.

14.4.4. Custodians must design applications and information systems to align with the enterprise architecture framework. Custodians must include security requirements in base architecture during information technology development, acquisition and deployment.

14.4.5. Systems that are no longer supported by the vendor will not be allowed to connect to the institution network without compensating controls approved by the office of the Information Security Officer.

14.4.6. Development, testing, and operational environments should be separate for all systems to reduce the risks of unauthorized access or changes to the operational environment.

14.5. **Vulnerability Management**

14.5.1. The System Administration and Institutions must establish procedures for vulnerability assessment and management, as failure to meet these

conditions could result in accidental or intentional acceptance of institutional risk by an unauthorized individual.

14.5.1.1. Vulnerability assessment and system patching will only be performed by designated individuals.

14.5.1.2. The System Administration and Institutions must create policy and procedures for vulnerability management that include acceptable time frames for addressing vulnerabilities and escalation procedures for handling unaddressed vulnerabilities.

14.5.1.3. The Information Security Officer will use vulnerability scanning tools to perform scans of information technology systems to identify information security vulnerabilities.

14.5.1.4. Custodians will identify vulnerabilities through active monitoring and review of third-party vulnerability sources for any old, new or unique vulnerabilities that currently exist.

14.5.1.5. The information security officer or designee is the only official authorized to perform, approve, and initiate vulnerability assessments or penetration tests.

14.5.1.6. The Information Security Officer or validated third party will conduct penetration tests that identify vulnerabilities that threat actors might exploit.

14.5.1.7. The Information Security Officer will check each vulnerability alert and patch release against existing systems and services prior to taking any action to avoid unnecessary remediation.

14.5.1.8. Information Security and Custodians shall evaluate and assign urgency for each vulnerability based on the intrinsic qualities of the vulnerability, the criticality of the business systems that it affects, and the sensitivity of the data that can be found on the specific assets as described in the Vulnerability Management Standard.

14.5.1.9. Custodians are responsible for remediating vulnerabilities identified during the vulnerability assessment process and through any other methodologies that reveal security weaknesses.

14.5.1.10. Custodians must remediate identified vulnerabilities within acceptable timeframes in order to prevent proliferation or escalation, and to prevent increases in risks to information and information resources. Vulnerabilities rated high risk must be addressed immediately.

14.5.1.11. The Information Security Officer will identify remediation options based on numerous risk factors including the availability of a patch and the risk accepted by utilizing a different method.

14.5.1.12. If remediation is not implemented custodians will:

14.5.1.12.1. Implement compensating controls;

14.5.1.12.2. Follow the risk management process; or

14.5.1.12.3. Pursue an exception.

14.5.1.13. Custodians must immediately update all configuration and inventory documentation to reflect applied remediation.

14.5.1.14. Custodians will consider vulnerability management as new systems and assets are deployed.

14.5.1.15. Before deploying a website or mobile application, the System Administration and Institutions must ensure language is included in third-party contracts that require the System Administration or Institution or an agreed-upon third-party to conduct vulnerability and penetration tests of the website or mobile application.

14.5.1.16. In lieu of facilitating a vulnerability or penetration test prior to deploying a website or mobile application, third parties may provide evidence to the Information Security Officer that testing of the current configuration of the website or mobile application compliant with the UNT System Information Security Handbook and applicable federal and state laws for protecting information resources and data security has occurred.

14.5.1.17. The System Administration and Institutions must inform third parties of the intention to conduct vulnerability and penetration tests in advance.

14.5.1.18. The System Administration and Institutions must obtain confirmation from third parties that they understand the requirement for conducting the vulnerability and penetration test and approve the actions in advance of deployment.

14.5.1.19. Custodians should monitor for end-of-life systems and applications to plan for mitigation and prevent future vulnerabilities.

14.5.1.20. Custodians must not block authorized network scan source IP addresses on the devices they support.

14.6. **Information System Maintenance**

14.6.1. The System Administration and Institutions must maintain a list of maintenance organizations and institutional personnel who are authorized to perform maintenance on multi-user information systems and develop procedures to ensure that:

14.6.1.1. Personnel performing maintenance on multi-user information systems have required access authorizations.

14.6.1.2. Designated personnel with required access authorizations and technical competence will supervise the maintenance activities of personnel who do not possess the required access authorizations.

14.6.2. Custodians are responsible for ensuring that preventative and routine maintenance is performed in a timely manner on information resources. Maintenance of information resources must be scheduled and documented.

14.6.3. Custodians must document and approve remote maintenance and diagnostic connections in advance.

14.6.4. Custodians must use strong authentication to establish remote maintenance and diagnostic connections.

14.6.5. Custodians shall terminate remote access and diagnostic connection upon completion of remote system maintenance.

14.6.6. Remote maintenance and diagnostic activities must be consistent with the other security policies in the handbook.

14.7. **System Planning and Acceptance**

14.7.1. The System Administration and Institutions shall establish policies and procedures ensuring that security reviews take place prior to contracting with external parties. The reviews must meet the requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, which includes signing of a non-disclosure agreement if confidential data will be used or shared as part of the agreement.

14.7.2. As part of the annual risk assessment process, the System Administration and Institutions shall require reviews of contracted third-party services to ensure continued compliance with agreed upon security and compliance standards.

14.8. **Reference**

14.8.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
14.8.2. International Standards Organization 27002:3; Information Systems Acquisition, Development, Testing, and Maintenance
14.8.3. International Standards Organization 27001:2013
14.8.4. Vulnerability Management Standard

15. Vendor Relationships

15.1. **Purpose**

System Administration and Institutions must establish procedures to manage vendor access to information and information resources.

15.2. **Information Security in Vendor Relationships**

Procedures to manage vendor access to information and information resources must include:

15.2.1. Identification of the types of vendors who may have access to institutionally owned information and information resources;

15.2.2. Standardized processes and lifecycle management for vendor relationships;

15.2.3. Processes for monitoring and controlling the access to information and information resources;

15.2.4. Cybersecurity awareness training at the beginning of contract terms as well as any renewal with completion tracked by Information Security.

15.2.5. Awareness for personnel involved in acquisitions regarding applicable policies, processes, and procedures; and awareness training for the organization's personnel interacting with vendor personnel regarding appropriate rules of engagement and behavior based on the type of vendor and the level of vendor access to the organization's systems and information.

15.3. **Security Requirements for Vendors**

15.3.1. Vendors acting as Users of Information Resources that are owned by the System Administration or Component Institutions must adhere to User responsibilities herein, including those found in Section 6.2.6 Users, Section 6.3 External Organization, and other sections of the handbook that are applicable to Users of Information Resources.

15.3.2. Vendors acting as administrators or Custodians of Information Resources that are owned by the System Administration or Component Institutions must adhere to the requirements of the latest version of NIST 800.53 regarding implementation of security and privacy controls for the information resources and information for which they have been given administrative or custodial responsibilities.

15.3.3. Vendors acting as providers of information technology systems or services that are provisioned for use by the System Administration or Component Institutions must adhere to the requirements of the latest version of NIST 800.53 regarding implementation of security and privacy controls for the information resources and information that the vendor is delivering to System Administration and Component Institutions.

15.3.4. Vendors acting as providers of Cloud Computing Services that are provisioned for use by the System Administration or Component Institutions must participate in and maintain program compliance and certification with the state of Texas risk and authorization management program, TX-RAMP, throughout the term of the contract. TX-RAMP is a standardized approach to the assessment and evaluation of cloud computing services. Texas Government Code § 2054.0593 mandates that state agencies as defined by Texas Government Code § 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services products entered or renewed on or after that date.

15.3.5. By entering into a written agreement with System Administration or Component Institutions that provisions access to information technology or

Cloud Computing Services vendors agree to maintain the confidentiality, integrity, and availability of information supplied by System Administration or Component Institution for which the vendor is providing the service.

15.3.6. Vendors that access information resources or information owned by System Administration and Institutions must complete security awareness training that is provisioned by the System Administration or Institution for which the vendor is conducting business. Training must be completed in the manner specified by the System Administration or Institution.

15.4. **Security Requirements for Vendors to Adhere to Prior to Initiation of Agreement or Contract with UNT System Administration or its Component Institutions.**

Vendors must do the following:

15.4.1. Complete and submit a security assessment of the technologies and services that will be provided to the System Administration or Institution prior to initiation of an agreement or contract.

15.4.2. Agree to implement remedial information security actions to adequately address non-compliance issues or risks identified by the System Administration or Institution during the risk assessment or technology review process.

15.4.3. Submit evidence that shows ability to meet or exceed State of Texas cybersecurity requirements identified in the Texas Cybersecurity Framework.

15.4.4. If providing a Cloud Computing Services, vendors must comply with the requirements of the state of Texas risk and authorization management program, TX-RAMP, if providing Cloud Computing Services to the System Administration and Institutions. TX-RAMP is a standardized approach to the assessment and evaluation of cloud computing services. Texas Government Code § 2054.0593 mandates that state agencies as defined by Texas Government Code § 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services products entered or renewed on or after that date.

15.4.5. Submit evidence of compliance with applicable federal and state data protection laws including, but not limited to, the following: Family Educational Rights and Privacy Act, Health Information Portability and Accountability Act, and Gramm-Leach-Bliley Act.

15.4.6. Submit evidence of compliance with federal and state laws regarding electronic and information resources accessibility requirements and agree to remediate accessibility deficiencies and gaps.

15.4.7. Provide evidence of compliance with payment card industry data security standards if processing payments, as applicable.

15.4.8. Provide evidence of adherence to Export Control laws, as applicable. Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR).

15.4.9. Provide copies of incident handling procedures and contingencies associated with supplier or vendor access including responsibilities of both the organization and suppliers.

15.5. **Security Requirements for Vendors After Initiation of Agreement or Contract with UNT System Administration or its Component Institutions.**

Vendors must do the following:

15.5.1. If providing a Cloud Computing Service, vendors must participate in and maintain compliance with the requirements of the state of Texas risk and authorization management program, TX-RAMP, if providing cloud services to System Administration and Institutions. TX-RAMP is a standardized approach to the assessment and evaluation of cloud computing services. Texas Government Code § 2054.0593 mandates that state agencies as defined by Texas Government Code § 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services products entered or renewed on or after that date.

15.5.2. Adhere to service level agreements identified in contractual and written agreements with the System Administration or Institution for which the vendor is providing a service or support.

15.5.3. Adhere to all applicable federal and state laws and data protection standards; including but not limited to: Family Educational Rights and Privacy Act, Health Information Portability and Accountability Act, Gramm

Leach Bliley Act, EU General Data Protection Regulation, and Payment Card Industry Data Security Standards.

15.5.4. Implement remedial information security actions to adequately address non-compliance issues or risks identified during risk assessment processes, as a requirement of TX-RAMP, and throughout the system development lifecycle.

15.5.5. Report data breaches to the Information Security Officer within 48 hours of discovery and provide evidence of remediation.

15.5.6. Provide evidence that information/data stored in third-party systems is recoverable and contingency plans are in place.

15.5.7. Conduct and provide evidence of vulnerability scanning and penetration testing for website and mobile applications that process and/or store confidential or personally identifiable information prior to deployment.

15.5.8. Provide evidence of the remediation of vulnerabilities identified through vulnerability scanning and penetration testing for website and mobile applications that process and/or store confidential or personally identifiable information prior to deployment.

15.5.9. Submit architectural designs of applications, information systems, and websites; and submit network/system diagrams of information systems in the context of the service that is being provided to System Administration and Institutions.

15.5.10. Provide authentication mechanisms for information systems and applications.

15.5.11. Provide administrator access levels to data that will be processed within information systems.

15.5.12. Provide data flow diagrams representing the flow of data within an information system.

15.5.13. Ensure that information systems provisioned for use by System Administration and Institutions are designed and configured to adhere to State of Texas requirements for secure architectural design.

15.5.14. Provide reports on security performance within the context of the services that are being provided to System Administration and Institutions.

15.5.15. Provide evidence of adherence to Export Control laws.

15.5.16. Return data and information resources upon termination of contract.

15.6. **Documentation Requirements for Initiating Vendor Relationships**

System Administration and Institutions must ensure that information security requirements are established for information and information resources prior to the initiation of a relationship with a vendor. Information security requirements should be documented and should include the following:

15.6.1. Explicit documentation of the access to information and information resources that will be granted to vendors for a particular engagement;

15.6.2. Language in vendor contracts requiring cybersecurity awareness training;

15.6.3. Processes and procedures for monitoring adherence to established information security requirements for each type of vendor and type of access, including third party review and product validation;

15.6.4. Controls established to ensure the integrity of the information or information processing provided by either party;

15.6.5. Incident handling procedures and contingencies associated with vendor access including responsibilities of both the organization and vendors;

15.6.6. Controls established to ensure the availability of the information or information processing provided by either party;

15.6.7. Conditions under which information security requirements and controls will be documented in an agreement signed by both parties; and

15.6.8. Procedures for managing the transition of information, information processing facilities and anything else that needs to be moved and ensuring that information security is maintained throughout the transition period;

15.6.9. Language in vendor contracts requiring the vendor to meet the security controls that the institution determines are proportionate with the institution's risk under the contract based on the sensitivity of the institution's data.

15.7. **Vendor Service Delivery Management**

System Administration and Institutions shall regularly monitor, review, and audit vendor service delivery and agreements. A service management relationship process should exist with the vendor and address the following:

15.7.1. Monitor service performance levels to verify adherence to the agreements;

15.7.2. Review service reports produced by the vendor and arrange regular progress meetings as required by the agreements;

15.7.3. Conduct audits of vendors, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

15.7.4. Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

15.7.5. Review vendor audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

15.7.6. Resolve and manage any identified problems;

15.7.7. Review information security aspects of the vendor's relationships with their vendors;

15.7.8. Ensure that the vendor maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster; and

15.7.9. Ensure that the vendor periodically provides evidence that it meets the security controls required under the contract.

15.8. **Changes to Vendor Services**

System Administration and Institutions shall document the process for managing changes to vendor services, including the following:

15.8.1. Changes to Vendor Agreements.

15.8.2. Changes made by the organization for implementing:

15.8.2.1. Enhancements to the current services offered;

15.8.2.2. Development of any new applications or systems;

15.8.2.3. Modifications or updates of the organization's policies and procedures; and

15.8.2.4. New or changed controls to resolve information security incidents and to improve security.

15.8.3. Changes in vendor services for implementing:

15.8.3.1. Changes and enhancements to networks;

15.8.3.2. Use of new technologies;

15.8.3.3. Adoption of new products or newer versions/releases;

15.8.3.4. New development in tools and environments;

15.8.3.5. Changes to physical location of service facilities;

15.8.3.6. Change of vendors; and,

15.8.3.7. Sub-contracting to another vendor.

15.9. **Reference**

15.9.1. International Standards Organization 27002:2013; Supplier Relationships
15.9.2. International Standards Organization 27001:2013
15.9.3. Texas Administrative Code, Title 1 § 202.77; Texas Risk and Authorization Management Program
15.9.4. Texas Risk and Authorization Management Program Manual

16. Information Security Incident Management

16.1. **Purpose**

Incident response procedures are necessary to ensure all staff understand their responsibilities for reporting incidents as well as to promote timely and thorough responses to incidents.

16.2. **Reporting Information Security Events and Weaknesses**

16.2.1. The System Administration and Institutions must establish information security incident management procedures that consider all phases of incident handling.

16.2.2. Custodians must investigate information security breaches promptly and report them to the Information Security Officer.

16.3. **Management of Information Security Incidents and Improvements**

16.3.1. Security incidents must be reported to the Information Security Officer in order to ensure appropriate handling of the incident.

16.3.2. In accordance with the requirements set forth in the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, the Information Security Officer will assess the incident, oversee incident response, assemble incident response teams as necessary, and will coordinate incident handling, remediation, reporting, and the authorization of forensic analysis as necessary. Custodians and Information Owners must cooperate with incident investigations.

16.3.3. Supervisors shall provide employees training for handling sensitive data and responding to incidents as appropriate for the employee's role.

16.3.4. An incident response resource reporting to the Information Security Officer shall assist and advise information system users in the handling and reporting of security incidents.

16.3.5. The Information Security Officer and Custodians shall employ automated mechanisms to increase the availability of incident response-related information and support.

16.3.6. As required by 1 TAC § 202.73 the Information Security Officer must report information security incidents to the Texas Department of Information Resources. Incidents that propagate to other state systems, result in criminal violations, involve unauthorized disclosure or modification of confidential information, or result in the compromise, destruction or alteration of information resources must be reported within 48 hours. Summary reports of incidents must be submitted monthly.

16.3.7. All personnel involved in incident handling must maintain confidentiality of incidents and associated activities during all phases of incident handling.

16.4. **Reference**

16.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

16.4.2. Texas Administrative Code, Title 1 § 202.73; Security Reporting

16.4.3. International Standards Organization 27002:2013; Information Security Incident Management

16.4.4. International Standards Organization 27001:2013

17. Business Continuity Management

17.1. Purpose

The System Administration and Institutions shall develop and maintain business continuity and disaster recovery plans for mission critical information resources. They shall also develop alternative procedures that enable personnel to continue critical day-to-day operations in the event of the loss of information resources.

17.2. Development of Business Continuity and Disaster Recovery Plans

17.2.1. Business continuity and disaster recovery plans must include a business impact analysis, risk assessment, and a disaster recovery plan as required by the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76. The business impact analysis determines which information resources are critical and should reflect information resource priorities based on the criticality of the resource, recovery time objectives, and recovery point objectives for data.

17.3. Requirements

17.3.1. Business continuity and disaster recovery plans must consider information security, should be tested at least annually, and shall be updated as frequently as needed.

17.3.2. Annual testing of redundant and high-availability information resources is required to ensure failover configurations work as intended.

17.3.3. The UNT System Vice Chancellor and Chief Information Officer must review and approve the business continuity plan for mission critical enterprise information resources. ISO 22301 is to be used for the framework for all business continuity plans to ensure consistency as required by ISO 27001.

17.3.4. The Information Security Officers for the System Administration and Institutions shall distribute business continuity and disaster recovery plans for information resources to key personnel and store a copy offsite.

17.3.5. The System Administration and Institutions must train employees in their contingency roles and responsibilities with respect to the information system and provide periodic refresher training as necessary.

17.4. **Reference**

17.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
17.4.2. International Standards Organization 27002:2013; Business Continuity Management
17.4.3. International Standards Organization 27001:2013
17.4.4. International Standards Organization 22301:2013; Societal Security -- Business Continuity Management Systems – Requirements

18. Compliance with Legal Requirements

18.1. **Purpose**

The System Administration and Institutions are required to identify and adhere to all legal, regulatory, contractual requirements, UNT System Regulations, System Administration Policies, and institutional Policies.

18.2. **Data Protection Laws**

All users must consider information protection laws and standards in regard to use of or access to information and information resources. Laws and standards include, but are not limited to, the following: Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), Texas Administrative Code 202 for higher education institutions, Texas Identity Theft Enforcement and Protection Act, Texas Medical Records Privacy Act, Payment Card Industry Data Security Standards, Digital Millennium Copyright Act, and intellectual copyright laws.

18.2.1. Information Owners and their delegates are responsible for identifying, documenting, and keeping up to date with all relevant legislative, statutory, regulatory, and contractual requirements relative to the information in their control. Custodians are responsible for implementing information security controls based on information protection laws and standards identified by owners

18.3. **Acknowledgement of Security Responsibilities**

All users of information and information resources of the System Administration and Institutions, including faculty, staff, students, guests, contractors, consultants, and vendors shall acknowledge and abide by the security controls governed by relevant legislative, statutory, regulatory, and contractual requirements.

18.4. **Information Systems Audit Considerations**

Information Owners, Custodians, and their delegates should ensure information systems and audit control activities involving verification of operational systems should be regularly planned and agreed upon to minimize risks and disruptions to business processes. The following guidelines should be observed during information systems audits:

18.4.1. Audit requirements for access to systems and data should be agreed upon with appropriate management.

18.4.2. The scope of technical audit tests should be agreed upon and controlled.

18.4.3. Audit tests should be limited to read-only access to software and data.

18.4.4. Information Owners, Custodians, and their delegates should allow read-only access for isolated copies of system files and should erase the files when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.

18.4.5. Information Owners, Custodians, and their delegates should identify and agree upon requirements for special or additional processing.

18.4.6. Information Owners, Custodians, and their delegates should run audit tests that could affect system availability outside business hours.

18.4.7. Information Owners, Custodians, and their delegates should monitor and log all access, where appropriate, to produce a reference trail.

18.5. **Reference**

18.5.1. International Standards Organization 27002:2013; Compliance with Legal Requirements

18.5.2. International Standards Organization 27001:2013

19. Privacy

19.1. **Purpose**

All users of information assets must protect the privacy of information assets according to governing laws, regulations, policies, and standards adopted and set forth by the UNT System and its component Institutions, including but not limited to: FERPA, HIPAA, and the Red Flags Rule.

19.2. **Responsibilities**

19.2.1. The UNT System Administration and Institutions must limit the collection, use, processing, and disclosure of personally identifying information and confidential information to that which serves to meet its function and purpose.

19.2.2. Custodians should restrict the use of personally identifying information and confidential information to the purpose for which it was collected.

19.2.3. Custodians should maintain accurate personally identifying information and confidential information and exhibit a reasonable effort to keep the information up to date.

19.2.4. Custodians should keep personally identifying information and confidential information no longer than necessary for processing as it was originally collected.

19.2.5. Custodians should process and protect personally identifying information and confidential information with security controls proportional to the information's confidentiality.

19.2.6. The information owner must provide consent prior to the processing of special kinds of personally identifying information and confidential information; including but not limited to genetic information, biometric information and health information.

19.2.7. Custodians shall not process personally identifying information and confidential information except under permissions granted by the Information Owner.

19.2.8. Employees, contractors, and other third parties must complete privacy awareness training prior to receiving access to institutional information assets.

19.2.9. The UNT System Administration and Institutions must obtain an individual's written or electronic consent before acquiring, retaining or disseminating information about an individual that identifies the individual or their location, including global position system technology, individual contact tracing, and biometric information except as required by law. The institution must maintain any records of consent agreements until the contract under which the information was acquired, retained or disseminated expires.

19.2.10. The Privacy Officer designated by the institution is accountable for developing, implementing and maintaining an institution-wide governance and privacy program in accordance with federal and state laws regarding the collection, use, maintenance, sharing and disposal of personally identifiable information by programs and information systems. The Privacy officer must coordinate activities with information owners and the information security officer to ensure that established practices and policies do not conflict with associated programs.

19.3. **Privacy and Institutional Websites**

19.3.1. The System Administration and Institutions must post the following on websites that process personally identifying information: The types of data collected when visiting the website; how collected information is used; how collected information is protected; and whether collected information is shared.

19.3.2. Custodians must conduct a transaction risk assessment prior to providing access to information or services on a website that requires personally identifying information. Web Developers must implement privacy and security safeguards on websites that transmit, collect or store personally identifying information.

19.3.3. Custodians must include links to the institution's Privacy policy on key website entry points.

19.3.4. Custodians must include the following text on websites: "By using or accessing a university website you consent to allowing the institution to collect identifiable information that includes unique electronic identification numbers, routing codes, network address, internet protocol address, and other information that is collected from your browser, device, or information that is provided by you during your use of the website."

19.3.5. The System Administration and Institutions must create and publish a privacy notice on all key public entry points or site policy pages that describes applicable provisions of the institutional privacy policy. The notice must meet all requirements of 1 TAC § 206.72.

19.4. **Reference**

19.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

20. General Security Exceptions

20.1. Purpose

The System Administration and Institutions shall implement procedures for granting and documenting security exceptions in accordance with 1 TAC §§ 202.71, 202.72, and 202.73. The Information Security Officer, with the approval of the institution of higher education head or his or her designated representative, may issue exceptions to information security requirements or controls. The Information Security Officer will coordinate exceptions and compensating controls with information and service owners. The Information Security Officer shall justify, document, and communicate any such exceptions as part of the risk assessment process. The Information Security Officer will provide an approval or rejection of a request for security exception to the custodial department. The Information Security Officer may revoke security exceptions at any time.

21. Sanctions for Violations

Penalties for violating the requirements of this handbook include but are not limited to disciplinary action, loss of access and usage, termination, prosecution, and/or civil action, as determined by UNT System Administration and Institutions.

Appendix A: System Administrator Code of Ethics

1. **Introduction**

   Certain designated persons are given broader access to the resources of information resources because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated information resources such as system maintenance, data management, and user support. The term "broader access" covers a range -from wider access than given to an ordinary system user, up to and including complete access to all information resources. Persons with the broadest (complete) access are sometimes called "superusers."

2. **Application**

   This code of ethics applies to all persons given broader-than-normal access to any information resources. It also applies to persons who authorize such access. The points contained in this code are considered additions to the responsibilities acknowledged by all ordinary information resources users and by the authorizers of information resources privileges.

3. **Responsibilities of Privileged Access Users**

   Superusers (individuals with full access to files) and all other persons given broader-than-normal access privilege to information resources agree:

   3.1. Not to "browse" through information while using the powers of privileged access unless such browsing is a specific part of their job description (e.g., an auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious, system-impairing behavior, and/or possible violations of policy; is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be done unless it is in the best interest of the institution.

   3.2. Not to disclose, to any unauthorized person, information observed while operating with privileged access.

   3.3. Not to copy any information for any purpose other than those authorized under their defined job responsibilities or pursuant to an authorized investigation or review.

   3.4. Not to intentionally or recklessly damage or destroy any information or information resource.

   3.5. Not to accept favors or gifts from any user or other person potentially interested in gaining access to information or information resources.

3.6. Not to do any special favors for any user, member of management, friend, or any other person regarding access to information or information resource. Such a favor would be anything that circumvents prevailing security protections or standards.

3.7. Not to disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.

3.8. Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.

3.9. Not to change or develop any information resources software in a way that would disclose information to persons not authorized to have it, or make it possible to retain any special access privilege once that authorized privilege has been terminated by management.

3.10. Not to make arrangements on information resources under their charge that will impair the security of other information resources. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.

3.11. Not to engage in any improper or deceptive financial practices.

3.12. Not to associate with malicious hackers, engage in or promote malicious activities that affect the confidentiality, availability or integrity of information and information resources.

Furthermore, superusers and all other persons given broader-than-normal access privileges on information resources agree that they will:

3.13. Report all suspicious requests, incidents, and situations regarding an information resource to the Information Security Officer and to institutional law enforcement.

3.14. Use all available software protections to safeguard information resources under their charge from unauthorized access by any person or other information resources.

3.15. Take steps to the best of their ability to comply with all information security standards and policies in force and furthermore, advise management and/or designated information security representatives of deficiencies in these standards.

3.16. Conduct themselves in a manner that will foster security awareness and understanding among users.

3.17. Respect the rights of intellectual property ownership by adhering to copyright laws and institutional policy.

3.18. Follow the requirements and limitations of software licenses. Never use software that is obtained or retained either illegally or unethically.

3.19. Only perform authorized actions on information resources and adhere to the user access agreement.

3.20. Conduct their work using good project management, incorporating quality practices, and providing full disclosure of risk.

3.21. Conduct themselves ethically and professionally in the execution of their job duties.

Appendix B: Handbook References

4. **Regulations**

   4.1. Texas Administrative Code, Title 1, Section 202

5. **Industry Guidelines**

   5.1. International Standards Organization 27001:2013
   5.2. International Standards Organization 27002:2013

6. **System Administration Policies, Regulations, and Publications**

   6.1. UNT System Regulation 06.1000 Information Security
   6.2. UNT System Information Ownership Guide
   6.3. Change Management Standard
   6.4. Vulnerability Management Standard

7. **Handbook Contributors**

Name	Title	Entity
Juan Serrano	Vice Chancellor and Chief Information Officer	UNT System Administration University of North Texas University of North Texas at Dallas
Richard Anderson	Chief Information Security Officer	UNT System Administration University of North Texas University of North Texas at Dallas
Paula Mears	Information Technology Security Analyst Lead	UNT System Administration University of North Texas University of North Texas at Dallas

Name	Title	Entity
Christine Sikes	Information Technology Compliance Analyst	UNT System Administration University of North Texas University of North Texas at Dallas
Jackie Thames	Senior IT Support Manager, HPS-IT Services	University of North Texas
Michael Baggett	Senior IT Support Manager, College of Visual Arts and Design	University of North Texas
Yonathan Khoe	Senior System Administrator, College of Visual Arts and Design	University of North Texas
Michael Hollis	Information Security Officer	University of North Texas Health Science Center
Patrick Hollar	Information Technology Support, Campus Technology Support Services	University of North Texas at Dallas
Daniel Garcia	Systems Administrator, Office of Information Tech	University of North Texas at Dallas

Appendix C: Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell	06/04/2014	
2	Charlotte Russell		Updated Texas Administrative Code References
3	Charlotte Russell	06/27/2016	Information Security Handbook Working Group Final Review Changes
4	Rama Dhuwaraha	07/13/2016	Chief Information Officer Revisions
5	Charlotte Russell	11/06/2017	Information Security Handbook Working Group Final Review Changes
6	Charlotte Russell	6/3/2019	Information Security Handbook Working Group Final Review Changes
7	Charlotte Russell	08/31/2020	Information Security Handbook Working Group
8	Charlotte Russell	12/8/2021	Revisions to Section 15: Vendor Relationship; Information Security Handbook Working Group Final Review Changes
		1/19/2022	Chief Information Officer Revision
9	Richard Anderson	10/1/2022	Chief Information Officer Revision